Vertraulich!
Bitte verschlossen weitersenden!

ERFINDUNGSMELDUNG
an Siemens AG bzw. Beteiligungsgesellschaft

Bereits vorab an CT IP übermittelt per FAX ☐
*Wenn ja - bitte **unbedingt** ankreuzen!*

Aktenzeichen der CT IP: 2002 E 17643 DE

Ich/Wir (Vor- und Nachname der/des Erfinder[s] - weitere Angaben und Unterschrift[en] letzte Seite)

Dr. Chris Winkler
Anton Schmitt
Johannes Bergmann

Anzahl der Erfinder: 3

Datum der Ausfertigung: 15.10.2002

melde[n] hiermit die auf den folgenden Seiten vollständig beschriebene Erfindung mit der Bezeichnung:

Verfahren zur Kopplung von Steuerkomponenten und Netzelementen in IP Netzen

I. An Vorgesetzten der/des Erfinder[s]

Eingang am:

Herrn/Frau Prof. C. Hoogendoorn — ICN WN CS FP (Dienststelle)

mit der Bitte, die nachstehenden Fragen zu beantworten:

a) Wann ging die Erfindungsmeldung bei Ihnen ein? → 22.10.2002

b) Geht die Erfindung auf öffentlich geförderte Arbeiten zurück?

☐ nein ☒ ja, Vorhaben: KING (BMBF GEFÖRDERT)

c) Gibt es ein zugehöriges internes FuE-Projekt?

☐ nein ☒ ja, Projekt: KING (WN CS FP)

Ab Eingang läuft gesetzliche Frist!

Nur bei CT-Erfindungen auszufüllen:

Projekt-Nr. _____ Titel: _____ Kerntechnologie: _____

☐ Entwicklungsprojekt ☐ Forschungsprojekt — im Interesse von Bereich: _____ Ansprechpartner: _____

d) Anmeldung wird empfohlen ☐ nein ☒ ja

Dringlichkeitsvermerk

Kosten trägt (Organisationseinheit): ICN WN CS

☐ Die Erfindung betrifft nicht unser Interessengebiet. Es sind noch folgende Dienststellen zu befragen: _____

23.10.2002 (Datum) — (Unterschrift des Vorgesetzten) CM Hoogendoorn

II. Bitte wegen gesetzlicher Frist sofort weiterleiten an

Eingang am:

Siemens AG
CT IP (Patentabteilung)

Standort: Mch P/Ri
(z.B.: Mch P/Ri, Erl S, Bln N, Khe R)

zur weiteren Veranlassung.

CT IPG AM Mch P/Ri
Eing. 24. Okt. 2002
GR
Frist

F: EMD V: 01.03.01 / B:Val

1. Welches technische Problem soll durch Ihre Erfindung gelöst werden?
Zukünftig werden IP-Netze neben den heute üblichen Internet- und Best-effort-Diensten auch höherwertige Qualitätsdienste transportieren und neue Anwendungen erlauben. Dazu sind Erweiterungen der Netzsteuerung z.B. zur Verwaltung der Netzressourcen oder für schnelle Rekonfiguration im Fehlerfall nötig. So werden z.B. im Projekt KING [1] dafür die Komponenten NAC (Network Admission Control) und NCS (Network Control Server) eingeführt.

Generell gibt es die Alternativen, Steuerkomponenten in die Netzkomponenten zu integrieren oder sie als eigene Server an die zu steuernden Netzkomponenten (Router) anzubinden (direkt oder über eine Netzverbindung). Die integrierte Lösung hat den Vorteil, dass der Steuerung durch die enge Kopplung zur Netzkomponente auch interne Informationen dieser Komponente zur Verfügung stehen. Demgegenüber ist eine „beigestellte" Lösung herstellerunabhängig und weitaus flexibler, da sie eben gerade nicht so eng mit den Interna der Netzkomponente verwoben ist. Darüber hinaus können "beigestellte" Lösungen auf standardisierten HW/SW Lösungen basieren, wohingegen Router meist auf proprietären HW/SW Lösungen basieren. Dies führt zu kürzeren Entwicklungszyklen und Kosteneinsparungen.

Am Beispiel einer Admission Control (AC) Steuerkomponente soll im folgenden die Problematik der Server-Lösung diskutiert und in Punkt 3. ein Verfahren angegeben werden, wie diese Probleme gelöst werden können.

Die Aufgabe einer Admission Control ist, ankommende Ressourcen Anfragen entgegenzunehmen, mit den noch verfügbaren Ressourcen abzugleichen und bei positivem Bescheid den Router am Netzrand (Netzkomponente Edge-Router) geeignet für die Kontrolle des Datenflusses zu programmieren (Einstellung von Funktionen wie marking, filtering, policing).

Dabei treten u.a. folgende zwei Fragestellungen (*) auf:
A) Wie erreichen die Ressourcen-Anfragen die beigestellte AC?
B) Wie kann die AC den Edge Router steuern/konfigurieren? Insbesondere: Woher bezieht sie die nötige Information über die Interna des Routers, z.B. welches Interface zu konfigurieren ist.

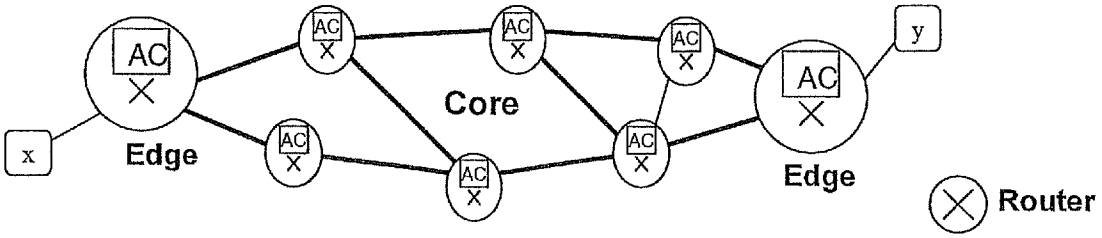
Im Prinzip existieren zwei Lösungsvarianten zum Auffinden der AC Komponente:
A) Der Datenpfad den die IP Pakete nehmen ist bekannt und entsprechend kann die AC Komponente direkt adressiert werden (Out-Band Signalisierung).
B) Das Signalisierungsprotokoll folgt dem Pfad der Datenpakete und findet so die AC Komponente automatisch (In-Band Signalisierung).
Im folgenden wird ausschließlich von der Signalisierung nach Variante B ausgegangen.

Das standardisierte Ressourcen Reservierungs-Protokoll RSVP [2] ist ein In-Band Signalisierungsprotokoll. Es löst die oben aufgezeigte Fragestellungen (*) wie unter 2. beschrieben (s.u.). Kernpunkt dabei ist, dass die RSVP-Instanz im Edge Router selbst implementiert wird und daher sehr eng mit dem Router und seinen Interna verzahnt operieren kann.

In dieser Erfindung wird ein Verfahren angegeben, wie separate Steuerinstanzen (hier am Beispiel einer AC-Instanz), an eine Netzkomponente (hier Edge-Router) angebunden werden können und dabei die o.g. Fragestellungen lösen.

2. Wie wurde dieses Problem bisher gelöst?
Im folgenden wird weiter das Beispiel einer AC Steuerkomponente exemplarisch betrachtet:

Das standardisierte Ressourcen Reservierungs-Protokoll RSVP [2] wird als Teil des Routers und seiner Steuerlogik implementiert.



Ab Beispiel eines RSVP-fähigen Netzes (also eines Netzes mit RSVP-fähigen Routern) mit zwei angeschlossenen Teilnehmern X und Y soll schematisch der Ablauf beschrieben werden:
X erzeugt eine Ressourcen-Anforderung an das Netz für seinen Datenstrom zu Y. Dabei muss sichergestellt werden, dass die Ressourcen-Reservierungen in den Routern auch tatsächlich entlang des späteren Datenpfades vorgenommen werden. In IP-Netzen hängt dieser Datenpfad vom aktuellen Routing ab. Daher wird in RSVP die Ressourcen-Anforderung mit der IP Zieladresse des Teilnehmers Y in das Netz gesendet und folgt damit automatisch dem Datenpfad des späteren Datenstroms zu Y.
Obwohl diese Nachrichten ja nun nicht an sie adressiert sind, müssen die RSVP Instanzen der auf dem Weg liegenden Router Kenntnis davon erhalten.
Daher sind diese Nachrichten durch den wohldefinierten IP-Protokoll-Typ „RSVP" im IP Header speziell gekennzeichnet. Die Router erkennen diesen Protokolltyp und geben solchermaßen gekennzeichnete Nachrichten direkt an ihre RSVP Instanz weiter.

Später im Verlauf der Prozedur muss die RSVP Instanz am Netzrand zu X „ihren" Edge-Router konfigurieren (filtering, marking, policing). Konkret ist dasjenige Interface zu konfigurieren, über das die RSVP Nachricht von X ursprünglich eingetroffen war und über das später der Datenstrom von X zu Y eintreffen wird. Da die RSVP Instanz im Router implementiert ist, kann sie diese internen Informationen abfragen.

Die Lösung für beide o.g. Probleme liegt hier in der engen Kopplung zwischen Router und Steuerinstanz:

A) Die Ressourcen-Anfragen erreichen die AC Instanz über spezielle Filter im Router, welche die Protokoll-ID erkennen und die Pakete am Routing vorbei direkt an die AC Instanz weiterreichen.
B) An die Information zu Konfiguration des Routers gelangt die AC-Instanz durch Zugriff auf Router-interne Datenbasen.

3. In welcher Weise löst Ihre Erfindung das angegebene technische Problem (geben Sie Vorteile an)?
In dieser Erfindung wird ein Verfahren angegeben, wie die o.g. Probleme auch bei losgelöst vom Router implementierten Steuerinstanzen, hier am Beispiel einer AC-Instanz, gelöst werden können.

A.) Wie erreichen die Ressourcen-Anfragen die AC?
Die Lösung für dieses Problem ist naheliegend und wird hier primär der Vollständigkeit halber angegeben. Aktuelle Router unterstützen sog. Policy-Routing, bei dem Regeln konfiguriert werden können, wie mit speziellen Paketen zu verfahren ist. In diesem Fall lautet die Regel:

> „Pakete mit einer bestimmten Protokoll-ID werden nicht einfach weiter-gerouted (zur Erinnerung: sie sind an den Teilnehmer Y adressiert), sondern an einen in der Regel eingestellten „next-hop" weitergeleitet, der zu der zuständigen externen Steuerinstanz führt."

Mögliche Varianten zur Anbindung der Steuerinstanz an den Router sind unter B) beschrieben.

B.) Woher bezieht die Steuerinstanz die zur Konfiguration nötigen internen Information?
Hier stellt sich das Problem, dass diese Information nicht von außen am Router abgefragt werden kann (z.B. enthalten die Routingtabellen des Routers nur Informationen über Ziele, jedoch nicht darüber, woher ein Paket kam).

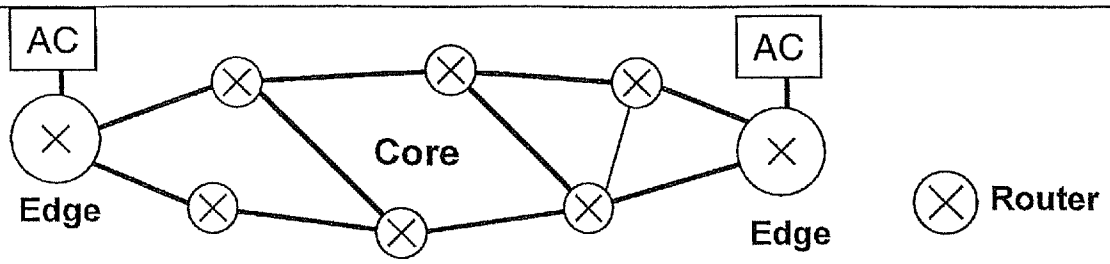
Inhalt dieser Erfindung ist, Router-interne Informationen, welche die Steuerinstanz zu Konfigurations- oder andere Zecken benötigt, dem Datenpaket (im Beispiel der Ressourcen-Anfrage) **an die Steuerinstanz mitzugeben, das Paket also mit dieser Information geeignet zu erweitern.**

Dies kann grundsätzlich auf zwei Arten geschehen:

1. auf eine mit den heutigen Routern darstellbare Weise
2. mit Modifikation der Router zur Unterstützung spezieller Kennzeichnungen/Paketerweiterungen

Ideal für eine rasche Einführung in die Netze sind Lösungen nach Variante 1.
Dafür werden im folgenden einige Ausführungsvarianten vorgeschlagen, die mit modernen Standard-Routern darstellbar sind.

1.) DSCP Marking
Voraussetzung: Steuerinstanz ist direkt an ein Interface des Routers angeschlossen, ihm also „beigestellt" (vgl. Bild, hier AC z.B. nur an den Edge-Routern).



Diese Lösung nutzt die Policy-Funktion moderner Router.

Bei Policy Routing kann in den Regeln neben einem next hop auch angegeben werden, welchen Wert das sog. DSCP Feld im IP Header (6 Bit) annehmen soll. Dieses dient in DiffServ-Netzen [3] zur Kennzeichnung der Paketpriorität. Bei direkter Kopplung der Steuerinstanz an den Router über ein eigenes Interface wird diese DSCP Information aber nicht benötigt.

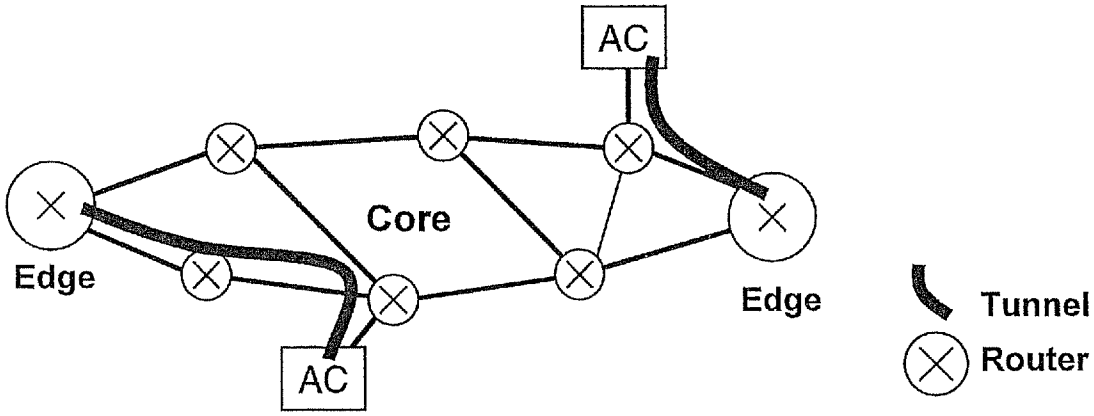
Daher kann auf jedem Eingangsinterface des Routers eine Regel konfiguriert werden, welche z.B. die Nummer des Interfaces oder andere Informationen in das DSCP-Feld codiert. Damit sind 64 Werte unterscheidbar und können dann von der Steuerinstanz adressiert werden.

Im Netz selber kann der DSCP Wert natürlich dennoch zur Kennzeichnung der Paketpriorität verwendet werden, da er z.B. von der Steuerinstanz auf einen anderen Wert gesetzt werden kann. Darüber hinaus kann, unabhängig von der „missbräuchlichen" Verwendung des DSCP-Priotitätsfeldes, das Paket im betroffenen Router selber mit einer wählbaren Priorität bearbeitet werden, da auch dies i.A. in die Router-Regel formuliert werden kann.

Werden mehr als 64 Werte benötigt, reicht das DSCP Feld allein nicht aus.

2.) Tunneling

Eine weitere Möglichkeit, wie ein Standard-Router Pakete kennzeichnen kann, sind IP-Tunnels, z.B. GRE-Tunnels [4]. Beim Tunneling wird das original IP Paket am Tunneleingang um einen Tunnelheader inclusive einer Tunnel-ID und einen neuen, also äußeren, IP Header ergänzt und mit diesem IP-Header durch das IP Netz gerouted. Am Tunnelendpunkt wird der äußere Header wieder entfernt und das Original-Paket weiter bearbeitet.



Moderne Router, insbesondere die hier betroffenen Edge Router, unterstützen oftmals eine oder mehrere Varianten des Tunneling.

Die Lösung mit Tunnels beruht darauf, dass mehrere Tunnels vom Router (Tunnelbeginn) zu der Steuerinstanz (Endpunkt) eingerichtet werden, die durch ihre Tunnel-ID (im Tunnel-Header) unterschieden werden können.

a) Nun kann als eine Variante die Tunnel-ID zur Übertragung interner Information verwendet werden, z.B. pro Interface ein eigene Tunnel eingerichtet werden, so dass die Interface-Nummer explizit oder implizit der Tunnel ID entspricht.
b) Genauso ist eine Kombination aus Tunnels und zusätzlicher Verwendung des DSCP-Marking (siehe 1.) möglich. Z.B. 2 Tunnels und DSCP-Marking zur Unterscheidung von z.B. 100 Werten.

Die Regeln auf den Interfaces enthalten dann als „next-hop" den entsprechenden Tunnel und ggf. ein DSCP-Marking.

Bei der Tunneling-Lösung entsteht darüber hinaus der Vorteil, dass die Steuerinstanz nicht direkt an den Router angebunden sein muss sondern irgendwo in das Netz gestellt werden kann (vgl. Bild). Sie ist dann über die

logische „Direkt-Schnittstelle" „Tunnel" erreichbar. In diesem Fall sollte ein DSCP Marking nach 1. auf dem inneren IP-Header vorgenommen werden, da dann der DSCP des äußeren Headers wirklich zur Prioritätskennzeichnung verwendet werden kann.

3.) MPLS

Eine andere Form des Tunneling ist MPLS [5]. Das Verfahren ist analog 2) nur dass an Stelle der IP Tunnels MPLS-„Tunnels" beziehungsweise – Pfade eingesetzt werden.

Mit der Idee, Router-interne Informationen, z.B. Interface-Nr. oder VPI/VCI-Nummern, durch geeignete Regeln im Router den Steuerpaketen hinzuzufügen wird es möglich, Steuerinstanzen vom Router losgelöst zu betreiben. Die dargestellten Ausführungsvarianten sind mit heutigen Routern realisierbar. Die Tunneling-Varianten erlauben dabei sogar, die Steuerinstanz irgendwo im Netz, also nicht unbedingt direkt am zu steuernden Router, aufzustellen.

Damit können flexible und Routerhersteller-unabhängige Lösungen zur Steuerung von Netzkomponenten dargestellt werden. Darüber hinaus basieren diese Lösungen auf standardisierter HW/SW, wohingegen Router meist auf proprietärer HW/SW basieren. Dies führt zu kürzeren Entwicklungszyklen und Kosteneinsparungen.

4. Worin liegt der erfinderische Schritt?

Mit dieser Idee können Steuerinstanzen, wie z.B. eine Admission Control Instanz, auch in heutigen IP Netzen ohne Modifikation der Router eingesetzt werden.

Der erfinderische Schritt liegt in der Lösung des Grundproblems über Kennzeichnung der Pakete sowie den zu heutigen Routern kompatiblen Ausführungsvarianten.

5. Ausführungsbeispiel[e] der Erfindung.

Implementierung im Rahmen der KING-Projekts

Referenzen

Nr.	Verfasser	Titel etc.
[1]	K. Schrodi	Basis Erfindungsmeldung(en) zu KING
[2]	IETF	RFC 2205 – RSVP
[3]	IETF	RFC 2474, RFC 2475 DiffServ
[4]	IETF	RFC 2784 GRE Tunneling
[5]	IETF	RFC 3031 MPLS

6. Zur weiteren Erläuterung sind als Anlagen beigefügt:

_____ Blatt der Darstellung eines oder mehrerer Ausführungsbeispiele der Erfindung;
(falls möglich, Zeichnungen im PowerPoint- oder Designer-Format anfertigen)

_____ Blatt zusätzliche Beschreibungen (z.B. Laborberichte, Versuchsprotokolle);

_____ Blatt Literatur, die den Stand der Technik, von dem die Erfindung ausgeht, beschreibt; *)

_____ sonstige Unterlagen (z.B. Disketten, insbesondere mit Zeichnungen der Ausführungsbeispiele):

*) Bitte Fotokopien oder Sonderdrucke aller zitierten Veröffentlichungen (Aufsätze vollständig; bei Büchern die relevanten Kapitel) mit vollständigen bibliographischen Daten beifügen.

7. Welche Dienststellen sind an der Erfindung interessiert? ICN WN

8. Wurde die Erfindung bereits erprobt (Durchführung von Versuchen, Anfertigung von Mustern)?

☐ nein ☒ ja, Ergebnis: Variante DSCP Marking wurde probiert und funktioniert

9. Für welche Erzeugnisse ist die Erfindung anwendbar?

Netzkomponenten in IP-Netzen, z.B.Next Generation Networks, SURPASS

10. Ist die Anwendung der Erfindung vorgesehen?

☐ nein ☒ ja, bei: Forschungsprojekt KING, KING-Demo, evt. auch Feldversuch

11. Ist ein auf der Erfindung beruhendes Erzeugnis geliefert oder ist eine Lieferung beabsichtigt?

☒ nein ☐ ja, (voraussichtlich) am _____ ; Bezeichnung des Erzeugnisses: _____

12. Ist eine Veröffentlichung der Erfindung beabsichtigt oder bereits erfolgt?

☒ nein ☐ ja, (voraussichtlich) am _____ in Buch, Zeitschrift: _____

13. Ist eine Mitteilung der Erfindung an Firmenfremde beabsichtigt oder bereits erfolgt?

☐ nein ☒ ja, (voraussichtlich) am 01.11.2002 an Im Rahmen des KING Projekts

14. Es wird gebeten, soweit möglich, die folgenden Kriterien abzuschätzen:

a Umgehungsschwierigkeit für Wettbewerber

Gleichwertige Alternativen

☐ praktisch nicht realisierbar

☒ erfordern Aufwand

☐ problemlos realisierbar

b Benutzungsattraktivität für Wettbewerber

Wettbewerberinteresse

☐ überragend

☐ durchschnittlich

☐ minimal

c Nachweis einer Wettbewerbernutzung

Benutzungsnachweis

☒ problemlos möglich

☐ aufwendig

☐ praktisch unmöglich

u Benutzung im Hause

☐ (voraussichtlich) ja

☒ offen

☐ unwahrscheinlich